Vulnerability Standards Update

Art Manion
amanion@cert.org
FIRST PSIRT TC 2018 Atlanta

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0275

About

Carnegie Mellon University

Software Engineering Institute (SEI)

- Federally Funded Research and Development Center (FFRDC)

CERT Coordination Center (CERT/CC)

Vulnerability Analysis

- Art Manion, Technical Manager/Principle Engineer
- Coordinated vulnerability disclosure
- Vulnerability discovery
  - Binary analysis
  - Fuzz testing
- Attack modeling
  - Ecosystem and data analysis
- Outreach, standards, policy

More about

Significant sponsorship

- Department of Homeland Security (DHS)
  - National Cybersecurity and Communications Integration Center (NCCIC)
    - US-CERT and ICS-CERT (different than CERT/CC)
- Department of Defense Cyber Crime Center (DC3)
  - DoD Vulnerability Disclosure Program (VDP) https://hackerone.com/deptofdefense

Coordination and disclosure: 1988

```
-----BEGIN PGP SIGNED MESSAGE-----


CA-88:01
                                CERT Advisory
                                December 1988
                            ftpd vulnerability
- ------------------------------------------------------------------------

   ** The sendmail portion of this advisory is superseded by CA-95:05. **

There have been several problems or attacks which have occurred in the
past few weeks.  In order to help secure your systems we have gathered
the following suggestions:

        1) Check that you are using version 5.59 of sendmail with the
           debug option DISABLED.  To verify the version try the following
           commands.  Use the telnet program to connect to your mail server.
           Telnet to your hostname or localhost with 25 following the host.
           The sendmail program will print a banner which will have the
           version number in it.  You need to be running version 5.59.
           Version 5.61 will be released on Monday 12/12/1988.  Any
           version less than 5.59 is a security problem.
```

Coordination and disclosure: 2017

Vulnerability Note VU#228519

Wi-Fi Protected Access (WPA) handshake traffic can be manipulated to induce nonce and session key reuse

Original Release date: 16 Oct 2017 | Last revised: 16 Nov 2017

Print Tweet Send Share

Overview

Wi-Fi Protected Access (WPA, more commonly WPA2) handshake traffic can be manipulated to induce nonce and session key reuse, resulting in key reinstallation by a wireless access point (AP) or client. An attacker within range of an affected AP and client may leverage these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocols being used. Attacks may include arbitrary packet decryption and injection, TCP connection hijacking, HTTP content injection, or the replay of unicast and group-addressed frames. These vulnerabilities are referred to as Key Reinstallation Attacks or "KRACK" attacks.

Summary

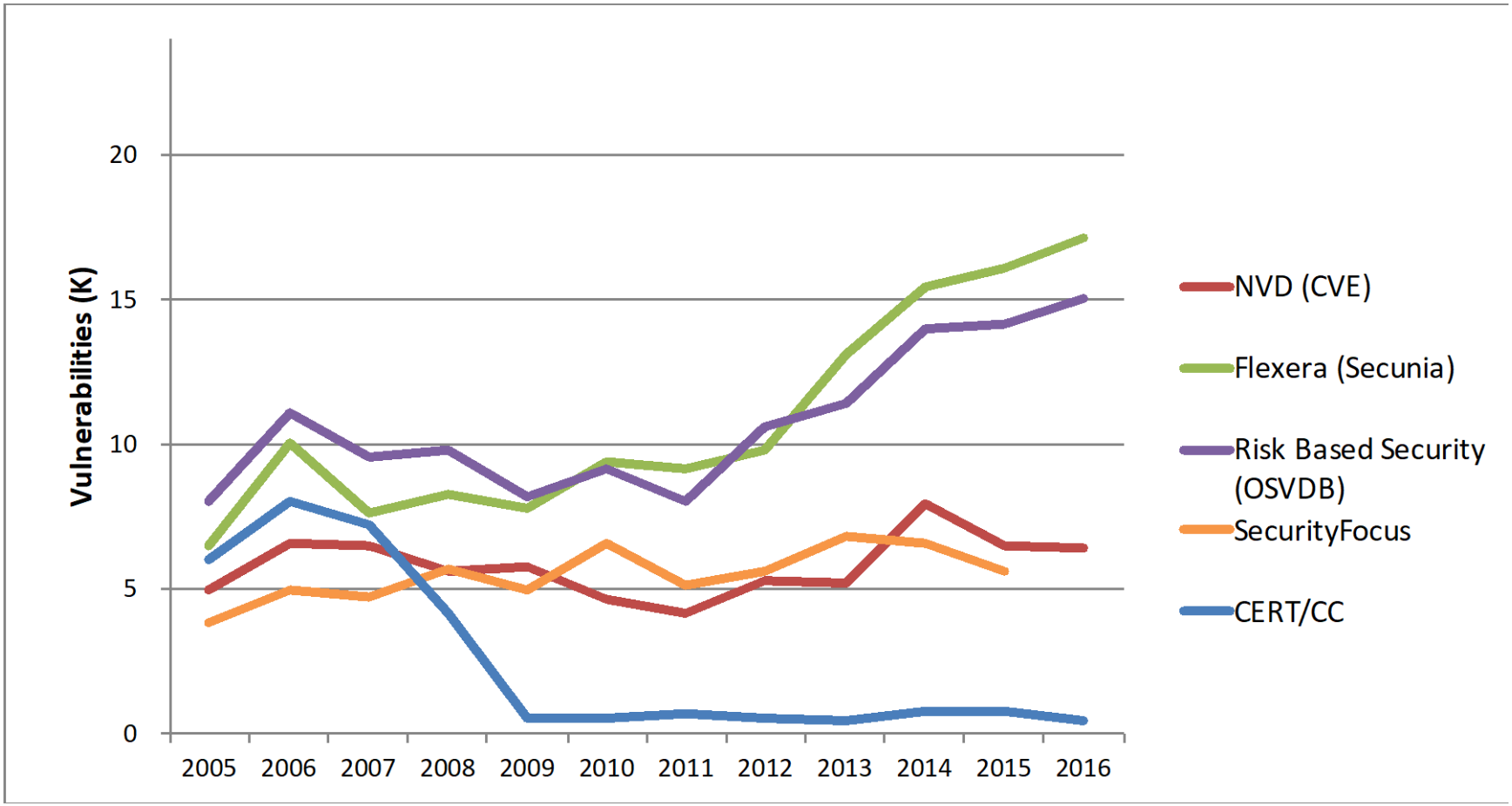
Standards, quasi-standards, formats, protocols, efforts

- Vulnerability information systems
- Policy, guidance, state of the practice

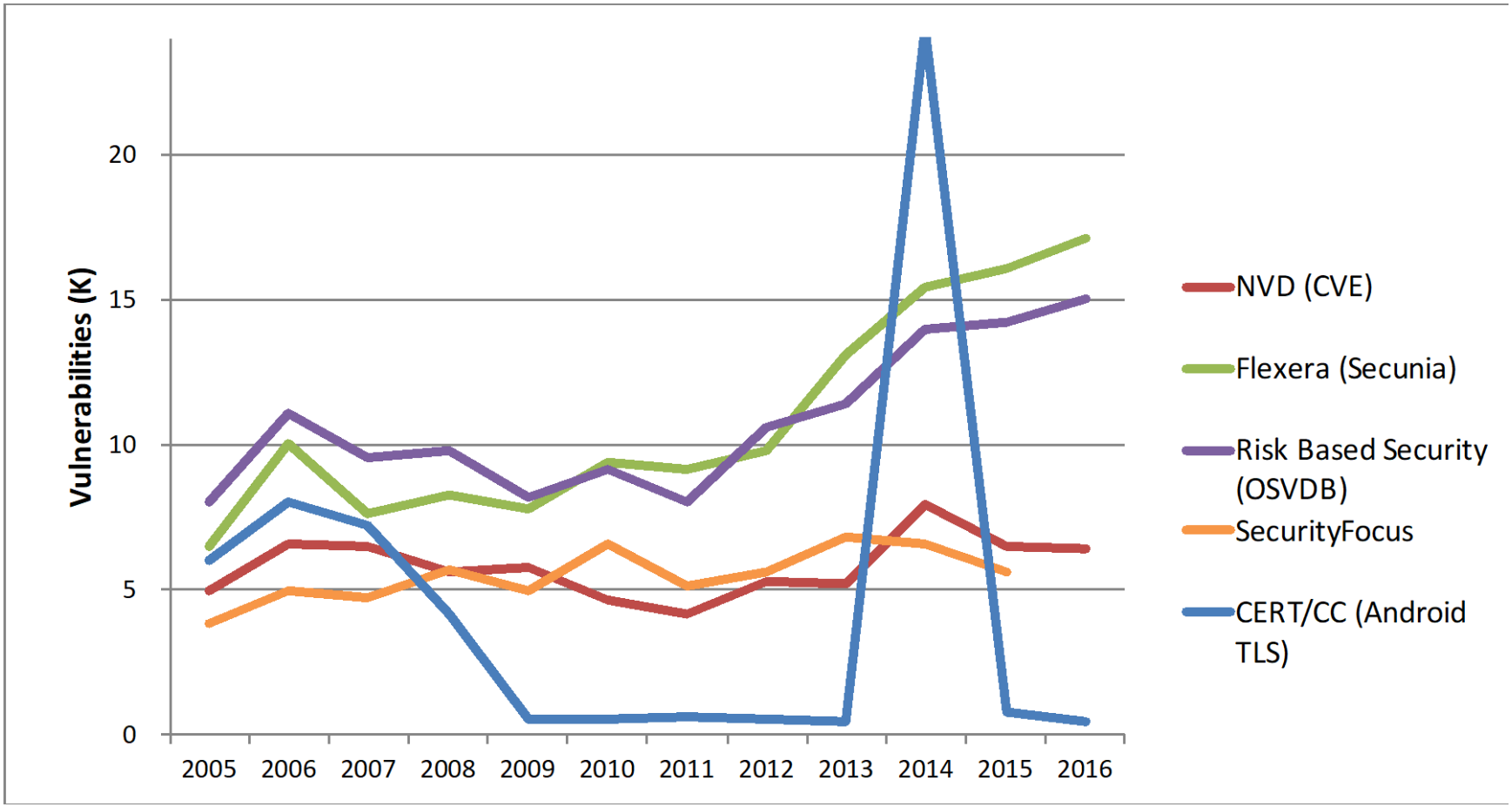
Sources

- Myself and CERT/CC
- FIRST VRDX-SIG

Vulnerability identification



Automated discovery



Vulnerability record

OASIS CSAF (CVRF)
https://www.oasis-open.org/committees/csaf/

CVE JSON
https://github.com/CVEProject/automation-working-group/tree/master/cve_json_schema

NIST NVD
https://nvd.nist.gov/vuln/data-feeds

NIST Vulnerability Description Ontology
https://csrc.nist.gov/publications/detail/nistir/8138/draft

Vendor contact

Vendor Contact record
FIRST Vulnerability Coordination SIG

A Method for Web Security Policies (security.txt)
https://tools.ietf.org/html/draft-foudil-securitytxt-03

CVE Numbering Authority (CNA) record
CVE Automation Working Group

Supply chain transparency

Software bill of materials (SBoM), manifest, inventory, supply chain, component relationships, third-party/OSS technical debt

Software Identification Tags (SWID)
https://tagvault.org/
https://www.iso.org/standard/65666.html
https://medisao.com/blog/automated-security-vulnerability-alerts-for-embedded-linux

Software Package Data Exchange (SPDX)
https://spdx.org/

Department of Commerce National Telecommunications and Information Administration (NTIA)

- Multistakeholder process rumblings

Managing Security Risks Inherent in the Use of Third-party Components
https://www.safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf

Supply chain transparency

OSS Security:That's Real Mature Of You!
https://www.first.org/conference/2017/program#poss-security-that-s-real-mature-of-you

H.R.5793 Cyber Supply Chain Management and Transparency Act of 2014

- "…bill of materials, of each binary component of the software, firmware, or product…"
- Not vulnerable (per NVD/CVE) or acceptance waiver
- "…designed in a manner that allows for any future security vulnerability or defect in any part of the software, firmware, or product to be easily patched, updated, or replaced…in a timely manner…"

(Vulnerability) information sharing

Using MISP to share vulnerability information efficiently
http://www.misp-project.org/2018/01/09/Using-MISP-to-share-vulnerability-information-efficiently.html

Trusted Automated eXchange of Indicator Information (TAXII)
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

TheHive Project
https://thehive-project.org

Traffic Light Protocol (TLP)
https://www.first.org/tlp/

Federacy
https://github.com/federacy/summary/

- "…a cryptoeconomic protocol and decentralized platform for security research and vulnerability management."

Severity

Common Vulnerability Scoring System (CVSS)
https://www.first.org/cvss/

- Vectors, severity function
- Severity, priority, risk
- Safety impact

Incomplete selection of less-used alternatives

- Parkerian Hexad
  http://www.computersecurityhandbook.com/csh4/chapter5.html
- Apgar
  https://en.wikipedia.org/wiki/Apgar_score
- Microsoft Exploitability Index
  https://technet.microsoft.com/en-us/security/cc998259.aspx
- DREAD
  https://blogs.msdn.microsoft.com/david_leblanc/2007/08/14/dreadful/
- Vulnerability Response Decision Assistance (VRDA)
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50301

Coordinated vulnerability disclosure

ISO/IEC 29147 Vulnerability disclosure and 30111 Vulnerability handling processes
https://www.iso.org/standard/45170.html
https://www.iso.org/standard/53231.html

PSIRT Services Framework
https://www.first.org/education/Draft_FIRST_PSIRT_Service_Framework_v1.0

NIST Cybersecurity Framework
https://www.nist.gov/cyberframework

- Version 1.1 Draft 2 RS.AN-5

CERT Guide to Coordinated Vulnerability Disclosure
https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure
https://www.first.org/global/sigs/vulnerability-coordination/multiparty/

…in collaboration with NTIA (US)
https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

Letters to Tech Companies on Meltdown and Spectre Vulnerabilities (US)
https://energycommerce.house.gov/news/letter/letter-tech-companies-meltdown-spectre-vulnerabilities/

Coordinated vulnerability disclosure

Global Forum on Cyber Expertise (GFCE) Coordinated Vulnerability Disclosure initiative (EU)
https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking

National Cyber Security Centre (NCSC-NL, NL)
https://www.ncsc.nl/english/security

More from NL
https://www.marietjeschaake.eu/media/uploads/posts/1520512095-Schaake%20cybersecurity%20act%20AM%20(final)%20COM(2017)0477_28-02-2018_10.53.58.pdf
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN

- “ensure that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates”
- “rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with”

Global Commission on the Stability of Cyberspace (EU)
https://cyberstability.org/

CEPS Software Vulnerability Disclosure in Europe (EU)
https://www.ceps.eu/content/software-vulnerability-disclosure-europe

Coordinated vulnerability disclosure

Food and Drug Administration (FDA, US)
https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

- NH-ISAC
- MD-VIPER
- MedISAO

National Highway Traffic Safety Administration (NHTSA, US)
https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity
https://www.nhtsa.gov/crash-avoidance/automotive-cybersecurity

- Auto-ISAC

Vulnerability Equities Process (VEP, US)
https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/

Coordinated vulnerability disclosure

Federal Trade Commission (FTC, US) enforcement actions

- "…respondent failed to…maintain an adequate process for receiving and addressing security vulnerability reports from third parties…" http://www.legis.ga.gov/legislation/en-US/Display/20172018/SB/315

A selection of draft bills in congress (US)

- Hack the DHS Act of 2017 (H.R. 2774)
- Promoting Good Cyber Hygiene Act of 2017 (H.R. 3202)
- Medical Device Cybersecurity Act of 2017 (S. 1656)
- Internet of Medical Things Resilience Partnership Act of 2017 (H.R. 3985)
- Hack Your State Department Act https://lieu.house.gov/sites/lieu.house.gov/files/LIEU_091_xml.pdf

CVD program before bounty!

Coordinated vulnerability disclosure

…missing from traditional “Protect my network” controls culture

- Center for Internet Security (CIS) Controls
- Information Systems Audit and Control Association (ISACA) COBIT
- NIST SP 800-53
- ISO/IEC 27000 series
  - 12.6.1 Technical vulnerability management
- IEC-62443 (ISA99) Industrial communication networks - Network and system security

Security research

DMCA exemption for good-faith security research (US)
https://www.federalregister.gov/documents/2015/10/28/2015-27212/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control#p-193

- "A motorized land vehicle"
- "A medical device…"
- "(including voting machines)"

Safe harbor (US)
https://hackerone.com/deptofdefense

- Covenant not to initiate legal action against researchers acting in good faith
- Make known that research activity was in good faith

"a new crime of unauthorized computer access" (US, GA)
http://www.legis.ga.gov/legislation/en-US/Display/20172018/SB/315

FIRST

Special Interest Groups (SIGs)
https://www.first.org/global/sigs/

- Vulnerability Coordination SIG
- Vendor SIG
- Vulnerability Reporting and Data eXchange (VRDX) SIG
  - Global Vulnerability Reporting Summit
    https://www.first.org/global/sigs/vrdx/summit2018/

PSIRT TC

- Atlanta, 2018
  https://www.first.org/events/colloquia/atlanta2018/